CHAPTER 7
FIRE AND SECURITY SYSTEMS

7-1. Fire and security system design criteria

The design of fire and security systems should be consistent with industry standards, such as those produced by NFPA and ANSI as well as applicable DoD guidelines and standards. Because the facility must meet applicable building codes, the AHJ, as defined by NFPA, should be consulted for any local or site-based design criteria.

a. In most cases, the applicable codes or the AHJ will require that a Nationally Recognized Testing Laboratory (NRTL), such as UL, approve the application of the equipment used to implement fire and security systems.

b. Integration of these functions with the SCADA system is typically not possible because the types of control equipment recommended by TM 5-601 for SCADA systems are not approved for fire and security applications. These functions usually require a separate system or systems.

7-2. General considerations

In the case of both fire and security, the system architecture should reflect the treatment of each peripheral zone as an independent building. The distributed processing systems used should provide for independent monitoring, alarm reporting, and alarm annunciation in each zone. As with the SCADA system, the command center should have a central operator station so that personnel there have full access to information from the zones. The security protocol of the mission and the life safety requirements of the architectural design of each zone dictate the detailed requirements for these systems within each zone; therefore, these requirements are not discussed here.

7-3. System layout

Figure 7-1 presents the architecture of a combined fire and security system for the example facility. Each zone has a fire and security field panel (FSFP) that provides complete local processing of monitoring, alarm and annunciation functions, operation of alarm-indicating appliances, and interface to zone HVAC systems.

a. Fire and security command consoles (FSCCs) are located at the public entry, which is assumed to have a staffed security station, and in the command center.

b. The network used to interconnect the FSFPs and FSCCs is typically proprietary to the equipment used. As shown in figure 7-1, the network should be redundant and provided with a means to isolate the segments within each zone in the event of a network fault, thus allowing the balance of the system to communicate freely.

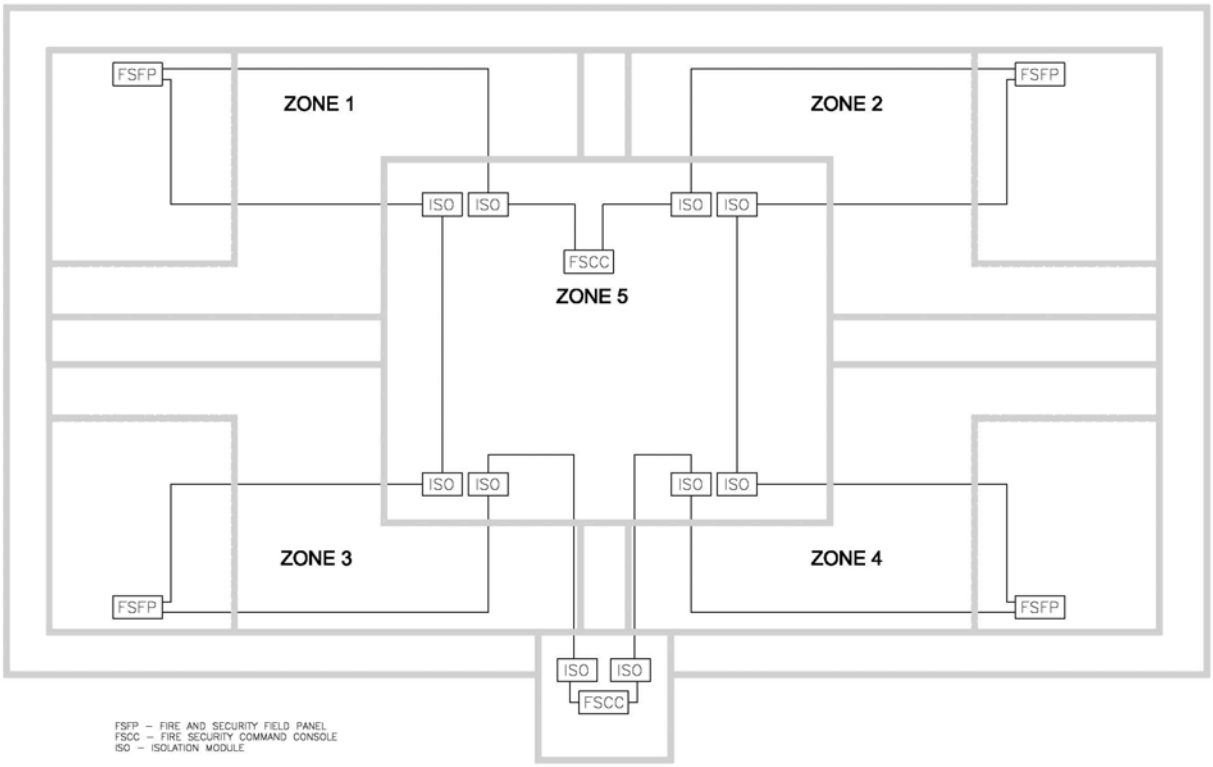

Figure 7-1. Fire and security system architecture

7-4. Interface to SCADA systems

Within each zone, the FSFP is directly interfaced to HVAC control systems, fire sprinkler systems, and any other systems that are necessary to provide the required performance. None of these interfaces, or the control actions that take place over them, should depend on the communication network or signals from other zones. Each FSFP should report a common zone alarm condition to the SCADA system PLC in that zone, which will relay it to the command center SCADA PLC.

a. A fire or security alarm within a peripheral zone will cause the command center PLC to isolate the command center from the utility sources served from that zone in anticipation of disruption or transient conditions in them.

b. Loss of communication to the FSFP in any zone, as detected by the FSCC in the command center, should also initiate preemptive isolation from that zone’s utility supplies.